обсягу роботи через впровадження МСФЗ зростанню заробітної плати бухгалтерів (а відповідно і небажання здійснювати додаткові види робіт); відсутність ефективно розробленої облікової програми відповідно до МСФЗ, яка б полегшила роботу бухгалтерів.

Список використаних джерел:
1.МСФЗ 13 «Оцінка справедливої вартості» / http://zakon3.rada.gov.ua/laws/show/929_068/paran2#n2
2. МСБО 39 «Фінансові інструменти: визнання та оцінка» / http://zakon3.rada.gov.ua/laws/show/929_015/paran474#n474

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

Ілляшенко О. В., *д-р. екон. наук, доцент,* ***Зачепа Б. О.,*** *магістр, Харківського національного університету міського господарства імені О. М. Бекетова*

Згідно Конституції України [1] забезпечення інформаційної безпеки є однією з найважливіших функцій держави, для виконання якої створюються системи захисту інформації (технічні, криптографічні, кібернетичні тощо) та управління безпекою. В Законі України “Про основи національної безпеки України” [2] йдеться “про основні сфери національної безпеки”, серед яких виокремлюється інформаційна. В Стратегії національної безпеки України [3] визначаються актуальні загрози національній безпеці, серед яких: загрози інформаційній безпеці; кібербезпеці та безпеці інформаційних ресурсів; безпеці критичної інфраструктури та основні напрями державної політики національної безпеки України і шляхи її забезпечення.

Особливої актуальності набувають питання досягнення інформаційної безпеки в банківських установах та адаптування національного законодавства з інформаційної безпеки до всесвітніх вимог. Підписання ІІ Базельської домовленості виявило нові закономірності у побудові діяльності фінансових установ. Серед нововведень виділяють необхідність створення резервів під операційні ризики банку. Впровадження в банківську діяльність системи управління операційним ризиком покликане зменшити втрати банку від некомпетентності персоналу, нестабільної роботи інформаційної системи та зовнішнього впливу, що сприяє банківській установі досягнути поставленої стратегічної мети з мінімальними фінансовими, ресурсними та інформаційними втратами.

У наукових колах тема інформаційної безпеки в банківських установах знаходиться в центрі постійної уваги, що підтверджується роботами таких авторів, як: Артеменко Д. А., Болгар Т. М., Адаменко С. І. [4-7]. Значна увага приділяється систематизації проблем забезпечення інформаційної безпеки банківських установ та шляхів їх вирішення. Розв`язок невирішених питань

реалізується через аналіз проблем в інформаційних системах банку, пошук протиріч в інформаційній системі.

Під інформаційною безпекою банку розуміється стан захищеності інформації про власників, керівництво, клієнтів банку, технологій та інформаційних ресурсів банку від внутрішніх і зовнішніх загроз. Забезпечення інформаційної безпеки є невід'ємною складовою частиною діяльності банку. Стан інформаційної безпеки банку визначається як уміння і здатність банку протистояти будь-яким спробам завдати шкоди законним інтересам банку.

Структуру інформаційної безпеки банківських установ становлять:

безпека інформаційних ресурсів;

безпека інформаційної інфраструктури;

безпека "інформаційного поля" підприємства.

Інформаційні ресурси банківської установи – це взаємопов'язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація, яка належить банківській установі. Відповідно безпека інформаційних ресурсів полягає в збереженні такої інформації від несанкціонованого поширення, використання і порушення її конфіденційності [5]. Безпека інформаційної інфраструктури полягає в такому стані захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, мереж електрозв'язку банківських установ, яка забезпечує цілісність і доступність інформації, що в них обробляється. Безпека "інформаційного поля" банківської установи складається в основному з несистематизованих потоків інформації, що оприлюднюються різними учасниками інформаційних відносин. Найбільш істотними загрозами безпеці інформаційних ресурсів є витік або втрата таких ресурсів (зокрема відомостей, що становлять банківську таємницю).

Загрози інформаційним ресурсам можуть бути реалізовані шляхом [6]:

підкупу осіб, які мають безпосередній доступ до банківської таємниці та іншої інформації з обмеженим доступом;

необережного, недбалого поводження з банківською таємницею та іншою інформацією з обмеженим доступом;

недотримання вимог щодо збереження інформації з обмеженим доступом при контактах з контролюючими та наглядовими органами в результаті правової та психологічної непідготовленості відповідальних працівників банківської установи і т. п.

Для захисту інформації банківські установи використовують різні заходи і засоби захисту. Заходи протидії несанкціонованому збору інформації в банку направлені на:

розробку відповідної нормативної бази, яка регулює режим і порядок доступу, зберігання і використання інформації банку;

контроль дотримання заходів інформаційної безпеки працівниками банку;

захист інформації в засобах і мережах її передачі та обробки.

Таким чином, забезпечення інформаційної безпеки банку – це система заходів щодо забезпечення необхідного рівня інформованості керівництва і персоналу банку, а так само зовнішнього середовища, ефективний захист всіх

видів інформації від зовнішніх і внутрішніх загроз, яка досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів і конкурентів, інформаційного аудиту та інформаційного моніторингу в банку, аналітичною обробкою інформації; організацією системи інформаційного забезпечення прийняття рішень керівництвом банку; визначенням категорій банківської інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідного режиму діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та їх нейтралізації.

Список використаної літератури:

1. Конституція України, 1996 / [Електронний ресурс] // – Режим доступу: http://zakon4. rada.gov.ua/laws/show/ 254к/96-вр – Назва з екрану.
2. Закон України Про основи національної безпеки України: Закон від 2003 / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon4.rada.gov.ua/laws/show /964-15 – Назва з екрану.
3. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ від 26.05.2015 / [Електронний ресурс] // РНБО – Режим доступу: №287/2015.http://zakon5.rada.gov.ua/laws/show/287/2015 – Назва з екрану.
4. Артеменко Д. А. Механізм забезпечення фінансової безпеки банківської діяльності: дис. канд. екон. наук / Д. А. Артеменко. – 2005.
5. Болгар Т. М. Проблеми фінансової безпеки вітчизняних банків в умовах ринкової трансформації економіки / Т. М. Болгар // Академічний обзор. - Дніпропетровськ: ДУЕП, 2007. – № 1. – С. 51-55.
6. Адаменко С. И. Характеристика и классификация угроз в банковской системе Украины / С. И. Адаменко // Стратегическая панорама. – 2004. − № 4. – С. 48−52.
7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон від 05.07.1994 № 81/94-ВР / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon5.rada.gov.ua/laws/show/80/94- вр/ed20111231 – Назва з екрану.

КАДРОВА БЕЗПЕКА В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКУ

Ілляшенко О. В., *д-р. екон. наук, доцент,* ***Путятіна О. С.,*** *магістр, Харківський національний університет міського господарства імені О. М. Бекетова*

Забезпечення кадрової безпеки банку та визначення її складових в Україні є на сьогоднішній день як у теоретичному, так і у практичному сенсі мало дослідженим питанням. Важкість дослідження кадрової безпеки банківської установи обумовлено низьким розвитком теоретичної бази дослідження даної категорії безпеки, значною кількістю її складових. Не існує цілісної концепції з питань управління кадровою безпекою, здатної забезпечити повне використання наявного кадрового потенціалу, протидіяти загрозам тощо.